أستكشاف أخطاء التطبيقات غير الخاصة بالمستعرض وإصلاحها في Umbrella

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء التطبيقات غير المستعرض وإصلاحها في Cisco Umbrella.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco Umbrella.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة

يوضح هذه المقالة أفضل الممارسات وخطوات أستكشاف الأخطاء وإصلاحها لتكوين تطبيقات ال تستخدم المستعرض للعمل باستخدام وكيل الويب الآمن ل Umbrella. في معظم الحالات، ال يلزم إجراء تغييرات في التكوين. ومع ذلك، ال تعمل بعض التطبيقات

بشكل جيد مع وظائف الأمان/الفحص (مثل فك تشفير SSL) ويجب إضافة إستثناءات لجعل وظيفة التطبيق باستخدام وكيل ويب. ينطبق هذا على Umbrella SWG بالإضافة إلى حلول وكيل الويب الأخرى.

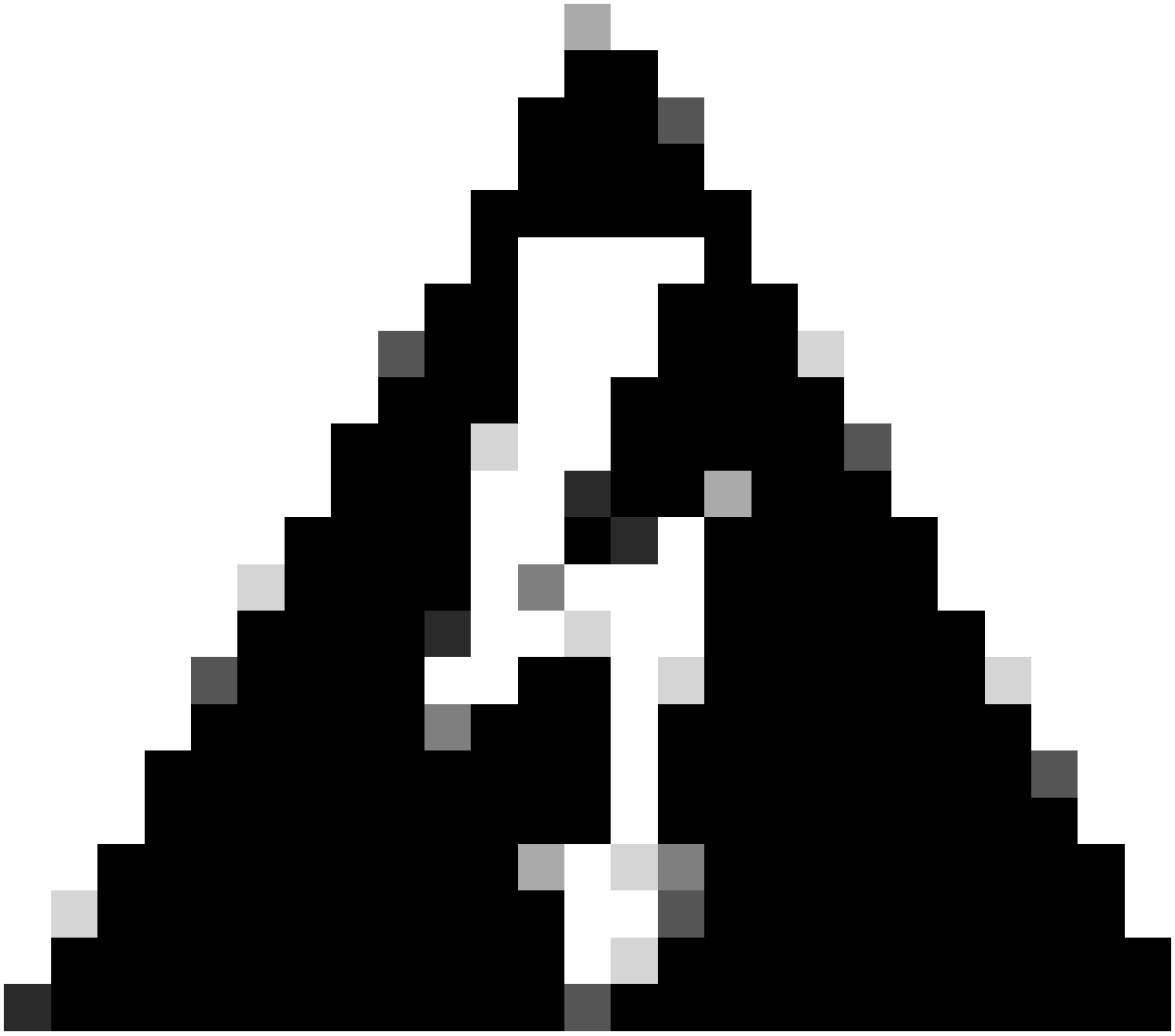
ويكون هذا مفيدا في الحالات التي يعمل فيها إصدار التطبيق من موقع الويب/المستعرض، ولكن إصدار التطبيق على سطح المكتب/المحمول لا يعمل.

مشاكل التوافق

يمكن أن تكون التطبيقات غير متوافقة لهذه الأسباب:

تثبيت Umbrella Root CA	يجب أن تكون Cisco Umbrella Root CA دائما موثوق بها لاتصالات TLS غير المنتظمة. • الحل: بالنسبة للتطبيقات غير الخاصة بالويب، تأكد من الثقة في جذر Cisco Umbrella في النظام / مخزن شهادات الجهاز المحلي مرجع مصدق.
تثبيت الشهادة	تثبيت الشهادة (PKP) هو عندما يتوقع التطبيق أن يتلقى وقوة دقيقة (أو شهادة CA) للتحقق من تأكيد تأكيد اتصال TLS. يتعذر على التطبيق قبول شهادة تم إنشاؤها بواسطة وكيل ويب والتوافق مع وظائف فك تشفير SSL. • الحل: تجاوز التطبيق أو المجال من فك تشفير SSL باستخدام قائمة فك تشفير انتقائية (راجع التحذير بعد الجدول) تتوفر هنا المزيد من التفاصيل حول التطبيقات المعروفة بتأثيرها على تثبيت الشهادات: تثبيت المفاتيح العام/تثبيت الشهادة
دعم إصدار TLS	يمكن أن يستخدم التطبيق إصدار / تشفير TLS قديم غير مدعوم من قبل SWG لأسباب أمنية. • الحل: تجاوز حركة المرور من أن يتم إرسالها إلى Umbrella باستخدام ميزة المجالات الخارجية (PAC / AnyConnect) أو إستثناءات VPN (النفق) (راجع التحذير بعد الجدول).
بروتوكول غير متعلق بشبكة الويب	تستخدم بعض التطبيقات بروتوكولات بخلاف HTTP (البروتوكولات) ولكنها لا تزال ترسل هذه البيانات عبر منافذ الويب الشائعة التي يتم اعتراضها بواسطة SWG. يتعذر على SWG فهم حركة المرور هذه. • الحل: راجع دور التطبيق لتحديد عناوين الوجهة / نطاقات IP المستخدمة بواسطة البرنامج. يجب إستبعاد هذا البرنامج من SWG باستخدام مجالات خارجية (PAC / AnyConnect) أو استبعادات VPN (Tunnel) (راجع التحذير بعد الجدول).
مصادقة	يتعذر على معظم التطبيقات غير المستعرض إجراء مصادقة SAML. لا توفر

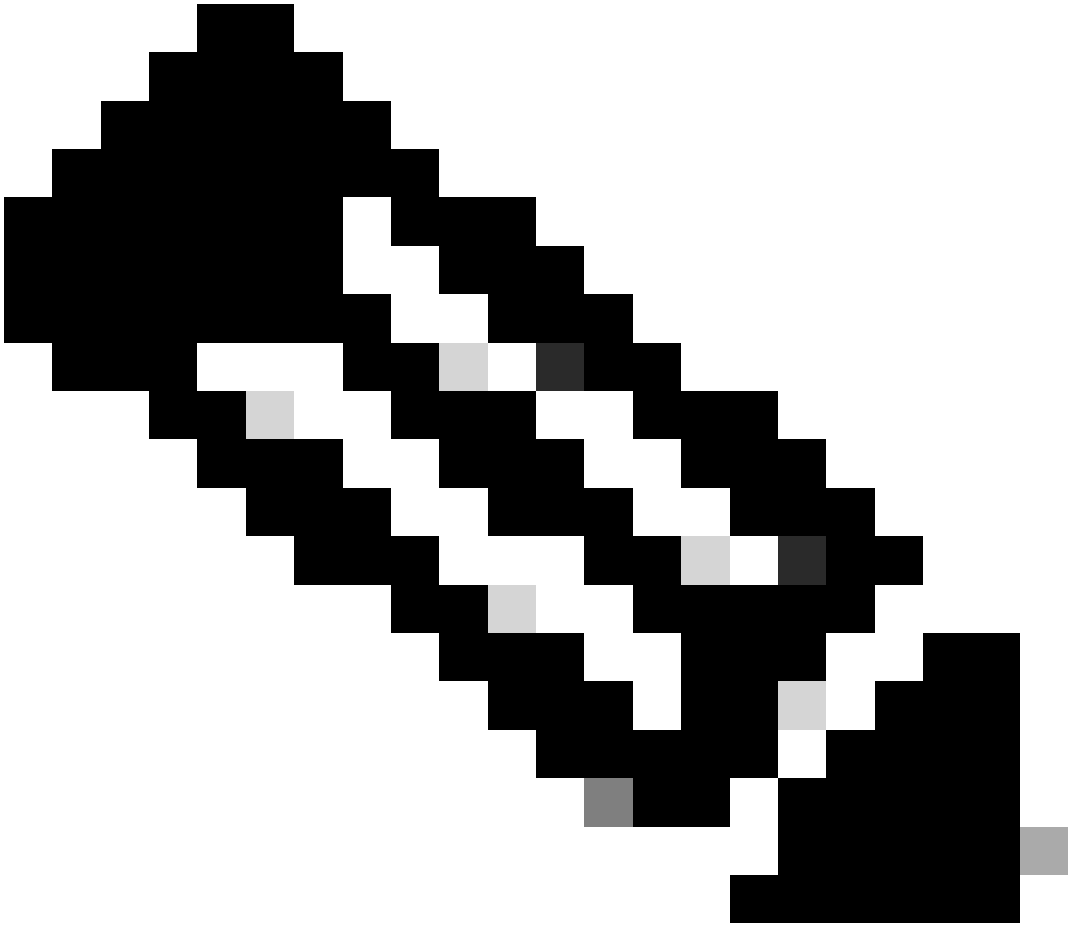
SAML	Umbrella تحدي تطبيقات غير المستعرض ل SAML وبالتالي ال يمكن أن تتطابق سياسات التصفية المستندة إلى المستخدم/المجموعة. • الحل: قم بتمكين ميزة بادئ IP حتى يمكن تخزين معلومات المستخدم مؤقتا للاستخدام مع التطبيقات غير الخاصة بالمستعرض. • البديل: السماح للتطبيق/المجال في قاعدة ويب استنادا إلى هويات الشبكة أو النفق (وليس المستخدمين/المجموعات).
تطلبات نطاق HTTP	تستخدم بعض التطبيقات طلبات HTTP Byte-range" عند تنزيل البيانات؛ يعني تنزل جزء صغير من الملف في كل مرة. يتم تعطيل هذه الطلبات لأسباب أمنية في SWG لأنه يمكن أيضا إستخدام هذا الأسلوب لتجاوز اكتشاف مكافحة الفيروسات. • الحل (https): تجاوز التطبيق أو المجال من فك تشفير SSL* في Umbrella باستخدام قواعد فك التشفير الانتقائية. • الحل (http): تجاوز التطبيق أو المجال من المسح الضوئي لبرنامج Anti-Virus* باستخدام قاعدة ويب مع خيار تجاوز الأمان. • البديل: اتصل بدعم Umbrella إذا كنت ترغب في تمكين طلبات Range بشكل افتراضي* لمؤسستك.
توافق الوكيل الصريح	تحترم بعض التطبيقات إعدادات وكيل النظام (على سبيل المثال. ملفات ال مسوغات الوصول المحمي (PAC) وتكون غير متوافقة بشكل عام مع بروكسيات الويب الصريحة. تقوم هذه التطبيقات بالتوجيه من خلال Umbrella SWG في ال نشر ملفات PAC. • الحل: يجب السماح بالتطبيق عبر جدار حماية الشبكة المحلية. راجع مواقع التطبيق للحصول على تفاصيل حول الوجهات/المنافذ التي سيتم السماح بها.



تحذير: يمكن أن يؤدي إنشاء هذه الاستثناءات إلى تعطيل وظائف فحص الأمان بما في ذلك المسح الضوئي لمكافحة الفيروسات، ومسح DLP، وعناصر تحكم المستأجر، والتحكم في نوع الملف، وفحص URL. قم بهذا فقط إذا كنت على دراية بالثقة في مصدر هذه الملفات. يجب موازنة إحتياجات الشركة للتطبيق مع تأثير الأمان الخاص بتعطيل هذه الميزات.

تطبيقات Microsoft 365

تستثني ميزة "التوافق مع Microsoft 365" تلقائيا عددا من مجالات Microsoft من وظائف "فك تشفير SSL" وإنفاذ السياسة. يمكن تمكين هذه الميزة لحل المشاكل المتعلقة بإصدار "سطح المكتب" من تطبيقات Microsoft. للحصول على مزيد من المعلومات، راجع [إدارة الإعدادات العمومية](#).

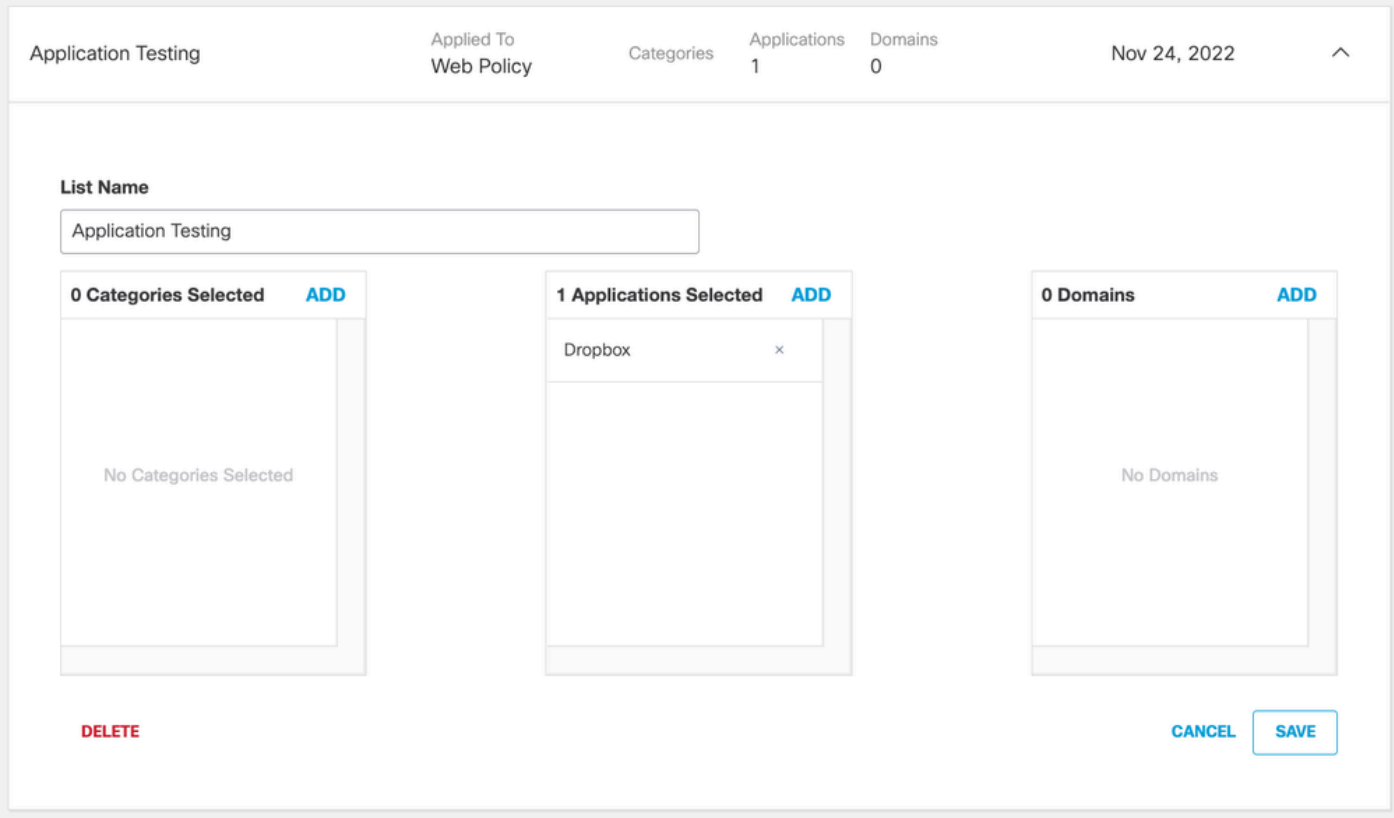


ملاحظة: لا تستثني ميزة التوافق لـ Microsoft 365 جميع مجالات Microsoft. تستخدم Umbrella توصيات Microsoft لقائمة المجالات التي يجب إستبعادها من التصفية. لمزيد من المعلومات، راجع فئات نقطة نهاية Office365 الجديدة.

تجاوز تثبيت الشهادة

تثبيت الشهادة (PKP) هو سبب شائع لمشكلات توافق التطبيقات. توفر Cisco قائمة شاملة بالتطبيقات المسماة التي يمكن تكوينها لتجاوز فك تشفير SSL للحل البديل. يمكن تكوين فك التشفير الانتقائي في السياسات > قواعد فك التشفير الانتقائي.

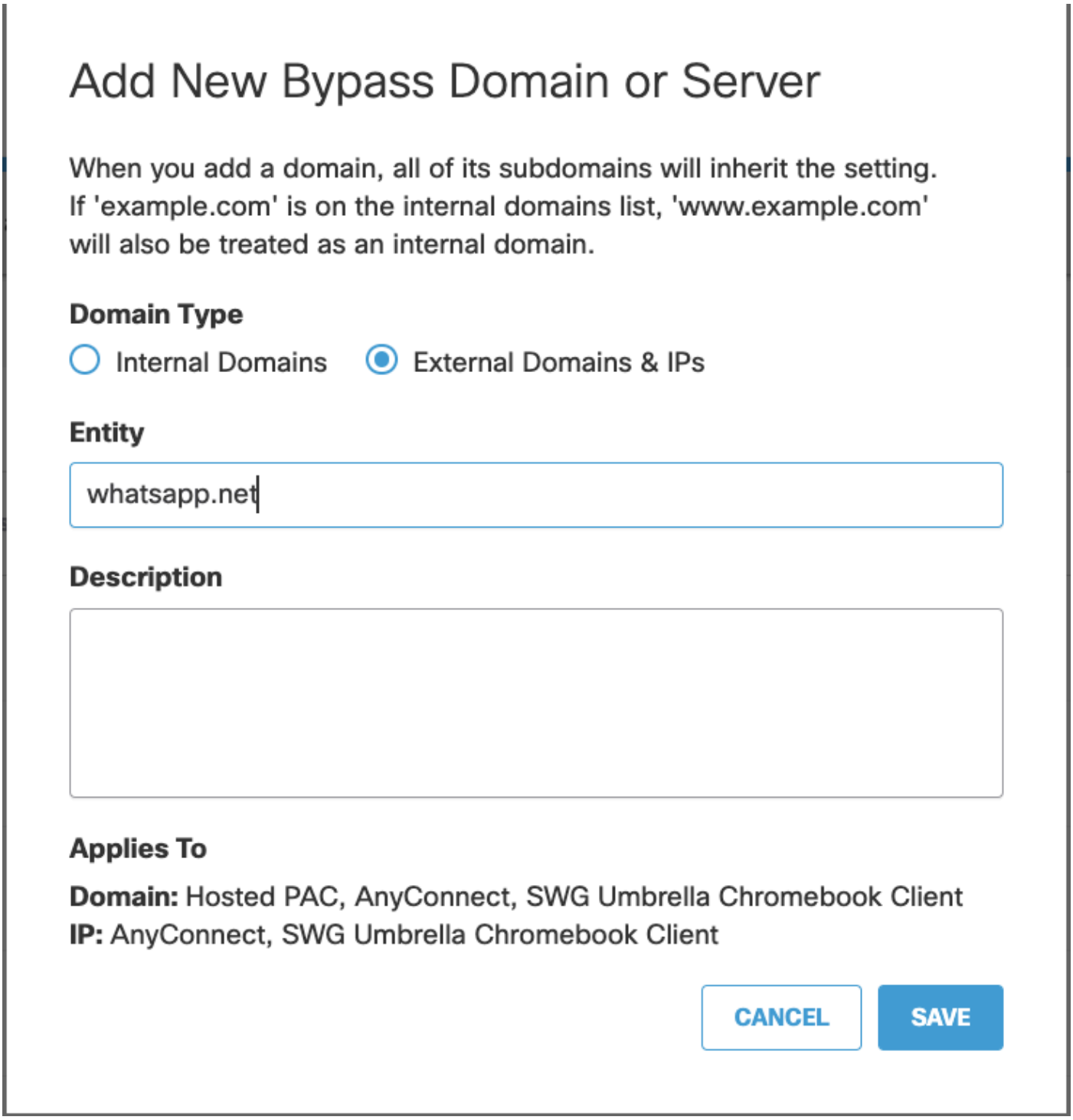
في معظم الحالات، يستطيع المسؤول حل مشكلات تثبيت الشهادة بمجرد إستبعاد التطبيق باسمه. وهذا يعني أنه يمكن حل هذه المشاكل دون الاضطرار إلى التعرف على قوائم المجالات أو الاحتفاظ بها.



بدلا من ذلك، يمكن تجاوز التطبيقات استنادا إلى مجال الوجهة/عنوان IP. اتصل بمورد التطبيق لتحديد قائمة المجالات/IPs القابلة للتطبيق أو راجع التعرف على الاستثناءات لإرساء الشهادة.

تجاوز توافق TLS

تعد إصدارات TLS القديمة أو المخصصة سببا مشتركا لمشكلات توافق التطبيقات. يمكن حل هذه المشاكل باستبعاد حركة مرور البيانات من Umbrella في عمليات النشر > إدارة المجال > المجالات الخارجية و IPs. في نشر النفق، يمكن إستثناء حركة مرور البيانات فقط بإضافة إستثناءات في تكوين VPN الخاص بك.



اتصل بمورد التطبيق لتحديد قائمة المجالات/IPs القابلة للتطبيق لاستبعاد أو راجع "تحديد إستثناءات إصدارات TLS غير المتوافقة" (فيما بعد في هذه المقالة).

أستكشاف الأخطاء وإصلاحها (متقدم)

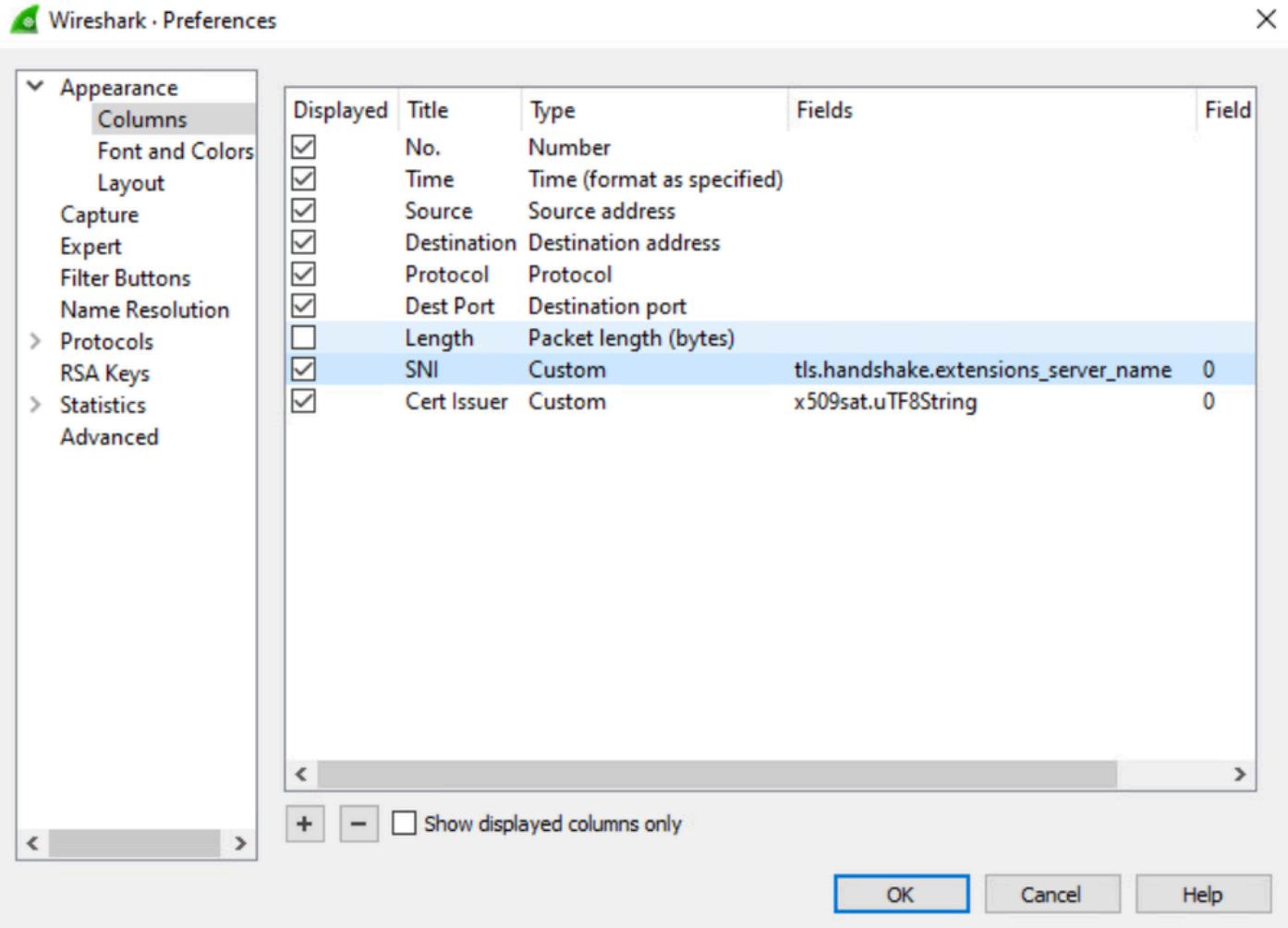
تستخدم التعليمات المتبقية في هذه المقالة مجموعات حزم Wireshark (www.wireshark.org) لأغراض أستكشاف الأخطاء وإصلاحها. يمكن أن يساعد Wireshark في تحديد المجالات التي تستخدمها التطبيقات للمساعدة في تنفيذ الاستبعادات المخصصة. قبل البدء، أضف الأعمدة المخصصة التالية في Wireshark:

1. تنزيل Wireshark من www.wireshark.org.

2. انتقل إلى تحرير > تفضيلات > أعمدة.

3. إنشاء أعمدة من نوع مخصص مع هذه الحقول:

```
http.host
tls.handshake.extensions_server_name
x509sat.uTF8String
```



لتنفيذ التقاط حزمة، أكمل هذه التعليمات أو راجع التقاط حركة مرور الشبكة باستخدام Wireshark.

1. تشغيل Wireshark كمسؤول.

2. حدد واجهات الشبكة ذات الصلة في Capture (التقاط) > Options (خيارات).

- لعمليات نشر مسوغات الوصول المحمي (PAC) / النفق، يمكنك التقاط واجهة شبكة LAN العادية لديك.
- بالنسبة لعمليات نشر AnyConnect، يمكنك التقاط واجهة شبكة LAN وواجهة الاسترجاع.

3. قم بإغلاق جميع التطبيقات الأخرى باستثناء التطبيق الذي يمثل مشكلة.

4. مسح ذاكرة التخزين المؤقت لـ DNS: `ipconfig /flushdns`

5. ابدأ التقاط Wireshark.

6. قم بنسخ القضية بسرعة ووقف إحتجاز Wireshark.

تحديد الاستثناءات لإرساء الشهادة

يتم فرض تثبيت الشهادة على العميل، مما يعني أن السلوك الدقيق وخطوات الحل تختلف لكل تطبيق. في إخراج الالتقاط، ابحث عن عالمات teltele التي تدل على فشل اتصال TLS:

- يتم إغلاق اتصال TLS بسرعة وأ إعادة تعيينه (RST أو FIN).
- تتم إعادة محاولة اتصال TLS بشكل متكرر.
- يتم إصدار شهادة اتصال TLS من قبل Cisco Umbrella وبالتالي يتم فك تشفيرها.

يمكن أن تساعد عوامل تصفية Wireshark هذه في عرض التفاصيل المهمة لاتصالات TLS.

النفق / AnyConnec

```
tcp.port eq 443 && (tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.rese
```

PAC / تقييد الوكيل

```
tcp.port eq 443 && (http.request.method eq CONNECT || tcp.flags.reset eq 1)
```

في هذا المثال، يتأثر تطبيق سطح المكتب DropBox بربط الشهادة عند محاولة الاتصال بـ client.dropbox.com.

(tls.handshake.extensions_server_name || tls.handshake.certificate || tcp.flags.reset eq 1 || tcp.flags.fin eq 1)

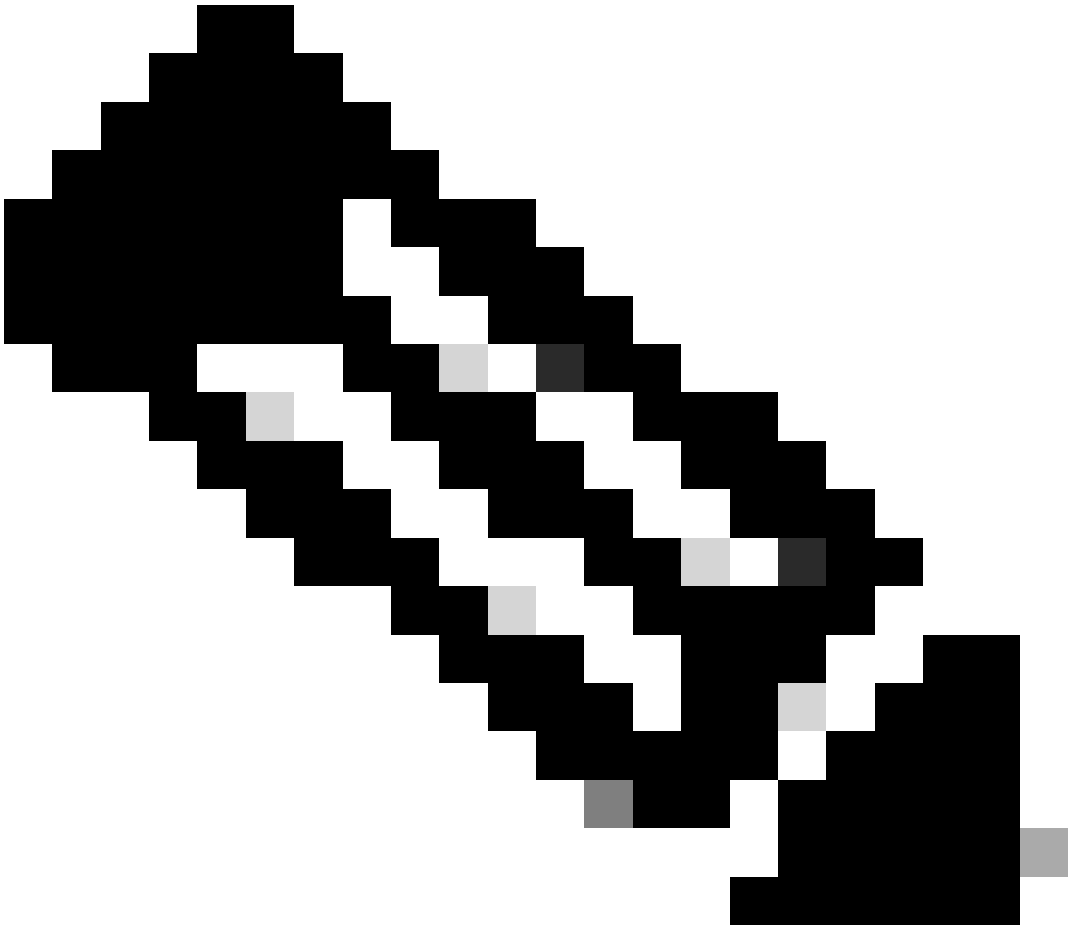
No.	Time	Source	Destination	Protocol	Dest Port	SNI	Info
281	43.038669	10.10.199.101	162.125.6.13	TCP	443		65148 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261120 Len=0
283	43.073849	162.125.6.13	10.10.199.101	TCP	65148		443 → 65148 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
287	43.083933	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
292	43.141656	162.125.6.13	10.10.199.101	TLSv1.2	65149		Certificate, Server Key Exchange, Server Hello Done
296	43.175867	10.10.199.101	162.125.6.13	TCP	443		65149 → 443 [FIN, ACK]
297	43.211415	162.125.6.13	10.10.199.101	TCP	65149		443 → 65149 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
306	46.361407	13.107.21.200	10.10.199.101	TCP	65123		443 → 65123 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0
309	46.458616	13.107.21.200	10.10.199.101	TCP	65125		443 → 65125 [FIN, ACK] Seq=32 Ack=1 Win=83 Len=0
315	48.228572	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
320	48.272897	162.125.6.13	10.10.199.101	TLSv1.2	65151		Certificate, Server Key Exchange, Server Hello Done
324	48.315138	10.10.199.101	162.125.6.13	TCP	443		65151 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
326	48.346412	162.125.6.13	10.10.199.101	TCP	65151		443 → 65151 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
330	48.357435	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
335	48.408976	162.125.6.13	10.10.199.101	TLSv1.2	65152		Certificate, Server Key Exchange, Server Hello Done
339	48.449204	10.10.199.101	162.125.6.13	TCP	443		65152 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
341	48.483947	162.125.6.13	10.10.199.101	TCP	65152		443 → 65152 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
345	48.514224	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
350	48.555627	162.125.6.13	10.10.199.101	TLSv1.2	65153		Certificate, Server Key Exchange, Server Hello Done
354	48.595411	10.10.199.101	162.125.6.13	TCP	443		65153 → 443 [FIN, ACK] Seq=297 Ack=3804 Win=261888 Len=0
356	48.631537	162.125.6.13	10.10.199.101	TCP	65153		443 → 65153 [FIN, ACK] Seq=3804 Ack=298 Win=43008 Len=0
360	48.641737	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
365	48.685384	162.125.6.13	10.10.199.101	TLSv1.2	65154		Certificate, Server Key Exchange, Server Hello Done
369	48.742518	10.10.199.101	162.125.6.13	TCP	443		65154 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261888 Len=0
370	48.779104	162.125.6.13	10.10.199.101	TCP	65154		443 → 65154 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
375	50.854534	10.10.199.101	172.217.15.110	TCP	443		64903 → 443 [FIN, ACK] Seq=2 Ack=74 Win=1020 Len=0
376	50.888092	172.217.15.110	10.10.199.101	TCP	64903		443 → 64903 [FIN, ACK] Seq=74 Ack=3 Win=83 Len=0
381	53.801686	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
387	53.845602	162.125.6.13	10.10.199.101	TLSv1.2	65156		Certificate, Server Key Exchange, Server Hello Done
390	53.888995	10.10.199.101	162.125.6.13	TCP	443		65156 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261120 Len=0
392	53.919018	162.125.6.13	10.10.199.101	TCP	65156		443 → 65156 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0
396	53.929107	10.10.199.101	162.125.6.13	TLSv1.2	44	client.dropbox.com	Client Hello
402	53.972689	162.125.6.13	10.10.199.101	TLSv1.2	65157		Certificate, Server Key Exchange, Server Hello Done
405	54.011019	10.10.199.101	162.125.6.13	TCP	443		65157 → 443 [FIN, ACK] Seq=473 Ack=3804 Win=261120 Len=0
406	54.047260	162.125.6.13	10.10.199.101	TCP	65157		443 → 65157 [FIN, ACK] Seq=3804 Ack=474 Win=43008 Len=0

Destination IP

Server Name

FIN Flag

Retries



ملاحظة: بعد إضافة الاستثناء (الاستثناءات) الضروري، يمكنك تكرار هذه الخطوات

عدة مرات لتعريف كل الوجهات المستخدمة من قبل التطبيق.

تحديد الاستبعاد لإصدارات TLS غير المتوافقة

ابحث عن إتصالات SSL/TLS التي لا تستخدم بروتوكولات TLS1.2+ الإلزامية المدعومة من قبل SWG Umbrella. يمكن أن يتضمن هذا بروتوكولات قديمة (TLS1.0 أو إصدار سابق) أو بروتوكولات مخصصة مفصلة يتم تنفيذها بواسطة تطبيق.

يوضح عامل تصفية المثال هذا حزم مصافحة TLS الأولية مع استعلامات DNS.

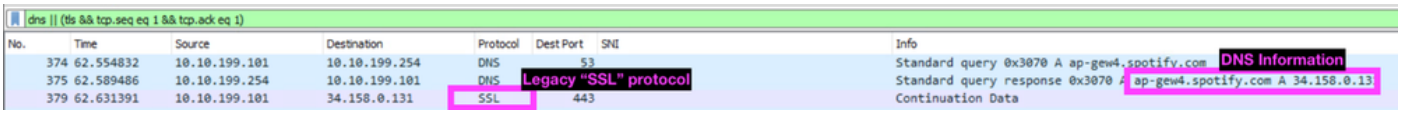
النفق / AnyConnect

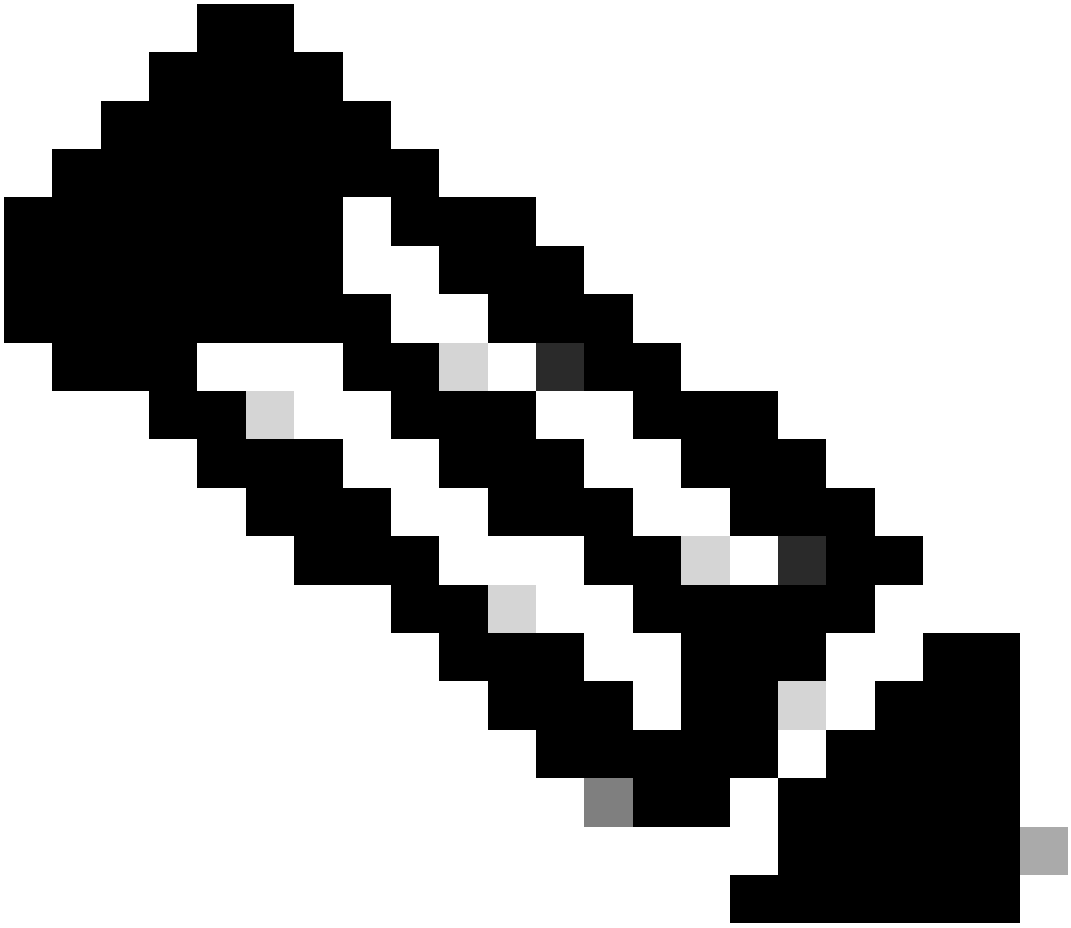
```
dns || (tls && tcp.seq eq 1 && tcp.ack eq 1)
```

PAC / تقييد الوكيل

```
dns || http.request.method eq CONNECT
```

في هذا المثال، يحاول تطبيق Spotify لسطح المكتب الاتصال ب ap-gew4.spotify.com باستخدام بروتوكول "SSL" غير قياسي وأ قديم ال يمكن إرساله عبر SWG.





ملاحظة: بعد إضافة الاستثناء (الاستثناءات) الضروري، يمكنك تكرار هذه الخطوات عدة مرات لتعريف كل الوجهات المستخدمة من قبل التطبيق.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).